Data Classification Standard

Responsible Office: Technology Services
Initial Approval: 02/06/2012
Current Revision Approved: 03/01/2022

Standard Statement and Purpose

This document provides the classification requirements for all data and information generated, processed, stored, transmitted, or used by all VCU faculty, staff, contractors, and third party business partners on behalf of VCU. This document is not intended to be used with data and information that is personally owned by individual employees, where if lost or stolen, has no negative impact on VCU.

This document is intended to be used by VCU Data Stewards to determine the sensitivity of the data used within their environment.

This document should be used in conjunction with the documents listed in the Related Documents Section.

Noncompliance with this Standard may result in disciplinary action up to and including termination. VCU supports an environment free from retaliation. Retaliation against any employee who brings forth a good faith concern, asks a clarifying question, or participates in an investigation is prohibited.

Table of Contents

Who Should Know This Standard

All persons that generate, store, process, transmit or handle VCU (university) data and information should read this standard and familiarize themselves with its contents and provisions. Additionally, all Trustees, Data Stewards, and Data Custodians should read and familiarize themselves with this standard and its contents and provisions.

Definitions

Category I Information/Data
Information protected under federal, state or industry regulations and / or other civil statutes, where if lost may require breach notification and cause potential regulatory sanctions, fines and damages to the institution's mission and reputation. (Confidential and Regulated data)

Category II Information/Data
All proprietary information that if improperly released has the potential to cause harm to the institution, its mission or its reputation, but does not require breach notifications, and security or privacy of such data is not regulated or required by law or contract. Such data includes proprietary and properly de-identified research information, business related email or other communication records, financial information, employee performance records, operational documentations, contractual information, intellectual property, internal memorandums, salary information, and all other information releasable in accordance with the *Virginia Freedom of Information Act (Code of Virginia 2.2-3700)*. (Sensitive data)

Category III Information/Data
All non-proprietary data that is considered publicly available for unrestricted use and disclosure, where if lost or illegitimately modified, these data will generate no negative impacts to individual departments, schools, colleges, or the institution as a whole. Such information is available to all members of the university community and to all individuals and entities external to the University community. Such data can make up public website information, public press releases, public marketing information, directory information, and public research information. (Public Data/Information)

Data Custodian
The data custodians are individuals or organizations (including third party vendors) who are responsible for entering, modifying and maintaining data in institutional, or third-party-provided information systems.

Data Handling
Data handling encompasses actions such as the generation, view, use, modification, deletion, or destruction of data. It also relates to the transfer or transmission of data from one location to another.

Data Steward
The data steward is a University director or equivalent position who oversees the capture, maintenance and dissemination of data for a particular operation. The data steward is responsible to

ensure data quality, develop consistent data definitions, sensitivity classifications, determine data aliases, develop standard calculations and derivations, define security requirements, document all appropriate “business rules” and monitor data quality within the source system and/or data warehouse. The data steward is also responsible for communicating data protection requirements to the data custodian; defining requirements for access to the data.

Data Trustee
Data Trustees are university officials who have the ultimate authority over policies, procedures, standards and guidelines regarding business definitions of data, and the access and usage of that data, within their delegated authority. Data trustees are responsible for appointing data stewards for the business domains (operational areas) within the institutional domains (subject areas) under their authority. Data trustees are high-level employees (e.g., vice presidents, vice provosts, and deans) appointed by and reporting to the President, including but limited to Provost and Senior Vice President of Academic Affairs, Vice President of Finance, Vice President of Administration, Vice President of Research, or Senior Vice President of Health Sciences.

Information Storage and Handling
Within the context of this document, information storage and handling refers to actions that create, store, transmit, process, modify, destroy, and / or archive information. The storage and handling of information may involve both electronic and physical actions.

Information Technology Baseline
An information technology baseline is a set of technical requirements that define the minimum required standard practices. Technology Baselines are used in conjunction with Technology Standards and Policies.

Information Technology Guideline
An information technology guideline is a recommended practice that allows some discretion or leeway in its interpretation, implementation, or use.

Information Technology Standard
An information technology standard is a formal document for an established norm of methods, criteria, and processes for technology subjects.

Third Party Business Partner
Within the context of this document, a third party business partner is a business entity that does business with VCU. Some but not all of VCU’s third party business partners will be handling VCU information. Some but not all of VCU’s third party business partners will be involved in the collection of data on VCU’s behalf or the storing, processing, and/or transmitting VCU information.

VCU Data and Information
Information in paper, electronic or oral form that is collected, generated, transmitted, processed or stored by a VCU employee, consultant, contractor or other affiliate in the course of their work and is used to support the academic, research, patient care or administrative operations at VCU.

Contacts

VCU Technology Services officially interprets this standard. The VCU Information Security Office (ISO) is responsible for obtaining approval for any revisions as required through the appropriate governance structures. Direct questions regarding this standard to the Information Security Office (infosec@vcu.edu).

Standard Requirements and Procedures

The following section contains the requirements of this standard.

A. Categorization of Data.

All VCU data and information that is generated, processed, stored or transmitted must be categorized as to its level of sensitivity in accordance with the specified classification levels; VCU data classification levels include **Category I** (Confidential and Regulated), **Category II** (Sensitive), and **Category III** (Public) information. Determining the classification of data can be done using the VCU Data Classification Tool.

B. Roles and Responsibilities.

The **VCU Data and Information Governance Policy** defines the roles, responsibilities, and expectations of Data Trustees, Stewards, and Custodians. Specific to this standard, Data Trustees, Stewards, and Custodians are responsible for the following:

1. **The Data Trustee is responsible for:**
    - Communicating effectively with Data Stewards to ensure the classification of data and definition of protection requirements.

2. **The Data Steward is responsible for:**
    - The identification of VCU IT systems in which their data is generated, processed, stored, and/or transmitted.
    - The determination of whether their data is subject to Federal or State regulatory requirements.
    - The determination of the level of potential harm of a compromise of the confidentiality, integrity or availability of each type of data handled by the IT system, and classify the sensitivity of the data accordingly.
    - The review and update of the classification level of VCU (University) data and information for changes in level of sensitivity on an annual basis or as changes occur.
    - Working with data trustees, custodians, and the information security office in defining protection requirements for data.

3. **The Data Custodian is responsible for:**
    - The selection of the types of data with which they need to work.
    - Reviewing and understanding the classification and protection requirements of the data types they selected.

- Adhering to the data management guidance / standards; including data protection requirements for the classified type of data.

4. **The University Information Security Office is responsible for:**
    - Providing guidance to VCU Data Stewards and Data Custodians for classifying VCU data/information.
    - The verification and validation of classification for VCU IT systems and data.
    - Working with Data Stewards, Data Trustees, and Data Custodians in defining protection requirements for data.
    - The communication of approved IT system and data classifications to Data Custodians and Data Stewards.

Forms

1. **VCU Information Security Exception Form**

Related Documents and Tools

The **Data Classification Tool** can be used to help an individual classify data and information in accordance with this standard.

The **VCU Information Technology Policy Framework** (https://ts.vcu.edu/askit/policies-and-publications/information-technology-policies-standards-baselines--guidelines/)
contains VCU Information Technology Policies, Standards, and Baseline requirements, all of which must be followed in conjunction with this standard.

Baseline documents can be found in the VCU University Computer Center IT Professionals Intranet under Security Baselines. Access to the IT Professionals Intranet requires approval. Requests for access can be made via email to uccnoc@vcu.edu.

Key policies are

1. Computer Network and Resources Use Policy
2. **Information Security Policy**
3. **Exposure and Breach of Information Policy**
4. **Network Management and Security Standard**
5. **Policies - Data and Information Governance**

Revision History

This standard supersedes the following archived policies and standards:

Approval/Revision Date	*Title*
02/06/2012	Data Classification Standard
09/06/2017	Revisions: Moved classification information to the data classification tool. Defined roles for data trustee, steward, and custodian, as well as the responsibilities for these groups and the information security office.
01/27/2022	Revisions: Added reference to Data and Information Governance policy. Revised responsibilities section to better align with the Data and Information Governance Policy. Reviewed for consistency and redundancy. Fixed broken links

FAQs

Q1. How do I classify my data?

A1. You can classify your data using the VCU Data Classification Tool.